PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-118876
(43)Date of publication of application : 07.05.1990

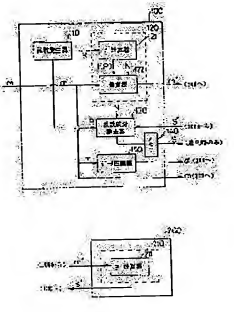
(51)Int.Cl. G06F 15/28

(21)Application number : 63-272608
(22)Date of filing : 28.10.1988

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : OTA KAZUO
OKAMOTO TATSUAKI

(54) ELECTRONIC BIDDING SYSTEM

(57)Abstract:
PURPOSE: To hold the secret of the corresponding relation of a bidding price except a successful bid and a tenderer even when an identity confirming person who is the sponsor side of the bidder and a bidding opening person conspire by providing a random number preparing device, a stirrer, a random number component remover and the like.
CONSTITUTION: A bidder supplies a random number R to a stirrer 120 by a random number preparing device 110 of a device 100 for a bidder and by using a bidding amount (m) and a publicized encipherment key N through an f-computer 121 and a multiplier 122 in the device 120, a stirred communication sentence m' is calculated. Next, the sentence m' is transmitted to a device 200 for an identity confirming person, a communication sentence s' with a signature corresponding to the sentence m' through a cirtifying device 210 is calculated, transmitted to the device 100, a signature value (s) corresponding to the amount (m) through a random component remover 130 is calculated and stored in a memory 140. Since the bidder supplies the amount (m) to a data compressor 150, a compression value (d) corresponding to the amount (m) is calculated, transmitted to the bidding opening person, the bidding opening person receives the compression value all bidders and after publicization, the bidder transmits the amount (m) to a device for opening a bidding, the unfair practice of a bidding promotor, the leakage of the bidding amount and the like can be prevented.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平2－118876

⑤Int.Cl.⁵　識別記号　庁内整理番号　⑬公開　平成2年(1990)5月7日
G 06 F 15/28　B　7165－5B

審査請求　未請求　請求項の数 3　（全11頁）

⑭発明の名称　電子式入札方式

⑳特　願　昭63－272608
㉒出　願　昭63(1988)10月28日

㉑発明者　太田　和夫　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内
㉑発明者　岡本　龍明　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内
㉑出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号
㉔代理人　弁理士　三好　保男　外1名

明細書の浄書(内容に変更なし)

明　細　書

1．発明の名称

電子式入札方式

2．特許請求の範囲

(1)開札者に対する複数の入札者からの入札を通信ネットワークを利用して電子的に行う電子式入札方式であって、入札者は入札額mの圧縮値αをα＝H（m）で作成して開札者に送信し、開札者はすべての入札者から圧縮値αを受信して公開し、入札者は圧縮値αの公開後に入札額mを開札者に送信し、開札者はすべての入札者から入札額mを受信すると、入札額mに対する圧縮値H（m）を算出してα＝H（m）が満たされることを検査してから受信したすべての入札額mを公開して落札額を決定し、これにより入札額mを公開する前に前記圧縮値H（m）を公開することで開札者が入札額mを見た後に入札できないようにしたことを特徴とする電子式入札方式。

(2)身元確認者によって身元を確認された複数の入札者からの開札者に対する入札を通信ネットワークを介して電子的に行う電子式入札方式であって、入札者は乱数発生器からの乱数成分および入札額mを攪乱器によって攪乱した入札額mに対応する通信文m′を作成して身元確認者に送信し、身元確認者は入札者の身元を確証した後に、攪乱された前記通信文m′を証明器に入力し署名付き通信文D（m′）を作成して入札者に返送し、入札者は前記署名付き通信文D（m′）から乱数成分の影響を除去して入札額mに署名を施した署名値D（m）を求めた後、入札額mに対応する圧縮値αをα＝H（m）で作成して開札者に送信し、開札者はすべての入札者からの圧縮値αを受信して公開し、入札者は圧縮値αの公開後に入札額mを開札者に送信し、開札者はすべての入札者から入札額mを受信すると、入札額mに対する圧縮値H（m）を算出してα＝H（m）が満たされていることを検査してから受信したすべての入札額mを公開して落札額moを決定し、落札額moを入札した入札者は落札額moに署名を施した署名

値D（ｍｏ）を開札者に送信し、開札者は該署名値D（ｍｏ）が落札額ｍｏに対する正しい署名であることを検査して落札者の身元が身元確認者によって承認され、かつ落札者が真に落札額ｍｏを入札したことを確認し、これにより身元確認者と開札者とが結託しても開札者が落札者以外の入札額と入札者との対応関係を知ることができないようにしたことを特徴とする電子式入札方式。

(3)身元確認者によって身元を確認された複数の入札者からの開札者に対する入札を通信ネットワークを介して電子的に行う電子式入札方式であって、身元確認者は初期応答文を入札者に送信し、入札者は該受信した初期応答文、乱数発生器からの乱数成分および入札額ｍに対する問い合わせ文β，β′を作成して身元確認者に送信し、身元確認者は前記初期応答文および前記受信した問い合わせ文に対応する応答文を証明器を用いて生成して入札者に返送し、入札者は前記応答文、前記乱数成分および前記問い合わせ文から乱数成分の影響を除去して入札額ｍに対応する署名値ｚ′を求めた後に、入札額ｍに対する圧縮値αをα＝Ｈ（ｍ）で作成して開札者に送信し、開札者はすべての入札者から圧縮値αを受信して公開し、入札者は圧縮値αの公開後に入札額ｍを開札者に送信し、開札者はすべての入札者からの入札額ｍを受信すると、入札額ｍに対する圧縮値Ｈ（ｍ）を算出してα＝Ｈ（ｍ）を満たすことを検査した後、受信したすべての入札額ｍを公開して落札額ｍｏを決定し、落札額ｍｏを入札した入札者は落札額ｍｏに対応する署名ｚ′，βを開札者に送信し、開札者は該署名ｚ′，βが落札額ｍｏに対する正しい署名であることを検査して、落札者の身元が身元確認者によって承認され、かつ落札者が落札額ｍｏを入札したことを確認し、これにより身元確認者と開札者とが結託しても開札者が落札者以外の入札額と入札者との対応関係を知ることができないようにしたことを特徴とする電子式入札方式。

3．発明の詳細な説明

［発明の目的］

（産業上の利用分野）

本発明は、通信ネットワーク上に分散配置された複数の入札者が電子的手段によって入札を行うプロトコルを実現する電子式入札方式に関する。

（従来の技術）

電気通信システムを用いた電子式入札、すなわちネットワーク上に分散配置された入札者が電子的手段によって競争入札する場合の入札プロトコルでは、入札額を他の入札者に秘密裏に開札者に届ける必要がある。この対策として、暗号化の手法が利用されている。また、通常の入札では、入札者と開札者が一同に会して入札・開札を行うので、開札者の不正は困難であると考えられている。しかしながら、電気通信を利用するときには、開札者と入札者が物理的に離れているので、開札者がその立場を悪用して落札額を不正に操作する恐れがある。この対策として、入札額に署名するディジタル署名の手法が利用されている。

従来、提案されている電子式入札方式としては、例えば山村三朗による「ネットワーク上における入札の一手法」（１９８８年暗号と情報セキュリティワークショップ講演論文集、ＷＣＩＳ８８－５，pp．４１－５０）に開示されたものがある。この山村氏の方式では、暗号通信とディジタル署名と同報通信とを組み合わせることにより上述した問題を解決している。

（発明が解決しようとする課題）

通常の入札では、入札額は開札者のみが知っており、他人に知られることはない。落札額以外の入札額は後日の商活動などに影響するので、知られる範囲を必要最小限にとどめることが好ましいものであるが、上述した山村氏の方法では、入札額が全員に知られてしまう問題がある。

本発明は、上記に鑑みてなされたもので、その目的とするところは、入札の主催者側である身元確認者と開札者とが結託したとしても落札額以外の入札額と入札者との対応関係を秘密にできる電子式入札方式を提供することにある。

［発明の構成］

（課題を解決するための手段）

上記目的を達成するため、本発明の電子式入札方式は、開札者に対する複数の入札者からの入札を通信ネットワークを利用して電子的に行う電子式入札方式であって、入札者は入札額mの圧縮値αを$\alpha=H(m)$で作成して開札者に送信し、開札者はすべての入札者から圧縮値αを受信して公開し、入札者は圧縮値αの公開後に入札額mを開札者に送信し、開札者はすべての入札者から入札額mを受信すると、入札額mに対する圧縮値H(m)を算出して$\alpha=H(m)$が満たされることを検査してから受信したすべての入札額mを公開して落札額を決定し、これにより入札額mを公開する前に前記圧縮値H(m)を公開することで開札者が入札額mを見た後に入札できないようにしたことを要旨とする。

また、本発明の電子式入札方式は、身元確認者によって身元を確認された複数の入札者からの開札者に対する入札を通信ネットワークを介して電子的に行う電子式入札方式であって、入札者は乱数発生器からの乱数成分および入札額mを攪乱器によって攪乱した入札額mに対応する通信文m'を作成して身元確認者に送信し、身元確認者は入札者の身元を確証した後に、攪乱された前記通信文m'を証明器に入力し署名付き通信文D(m')を作成して入札者に返送し、入札者は前記署名付き通信文D(m')から乱数成分の影響を除去して入札額mに署名を施した署名値D(m)を求めた後、入札額mに対応する圧縮値αを$\alpha=H(m)$で作成して開札者に送信し、開札者はすべての入札者からの圧縮値αを受信して公開し、入札者は圧縮値αの公開後に入札額mを開札者に送信し、開札者はすべての入札者から入札額mを受信すると、該入札額mに対する圧縮値H(m)を算出して$\alpha=H(m)$が満たされていることを検査してから受信したすべての入札額mを公開して落札額m_0を決定し、落札額m_0を入札した入札者は落札額m_0に署名を施した署名値D(m_0)を開札者に送信し、開札者は該署名値D(m_0)が落札額m_0に対する正しい署名であることを検査して落札者の身元が身元確認者によって承認され、かつ落札者が真に落札額m_0を入札したことを確認し、これにより身元確認者と開札者とが結託しても開札者が落札者以外の入札額と入札者との対応関係を知ることができないようにしたことを要旨とする。

更に、本発明の電子式入札方式は、身元確認者によって身元を確認された複数の入札者からの開札者に対する入札を通信ネットワークを介して電子的に行う電子式入札方式であって、身元確認者は初期応答文を入札者に送信し、入札者は該受信した初期応答文、乱数発生器からの乱数成分および入札額mに対する問い合わせ文β, β'を作成して身元確認者に送信し、身元確認者は前記初期応答文および前記受信した問い合わせ文に対応する応答文を証明器を用いて生成して入札者に返送し、入札者は前記応答文、前記乱数成分および前記問い合わせ文から乱数成分の影響を除去して入札額mに対応する署名値z'を求めた後に、入札額mに対する圧縮値αを$\alpha=H(m)$で作成して開札者に送信し、開札者はすべての入札者から圧縮値αを受信して公開し、入札者は圧縮値αの公開後に入札額mを開札者に送信し、開札者はすべての入札者からの入札額mを受信すると、入札額mに対する圧縮値H(m)を算出して$\alpha=H(m)$を満たすことを検査した後、受信したすべての入札額mを公開して落札額m_0を決定し、落札額m_0を入札した入札者は落札額m_0に対応する署名z', βを開札者に送信し、開札者は該署名z', βが落札額m_0に対する正しい署名であることを検査して、落札者の身元が身元確認者によって承認され、かつ落札者が落札額m_0を入札したことを確認し、これにより身元確認者と開札者とが結託しても開札者が落札者以外の入札額と入札者との対応関係を知ることができないようにしたことを要旨とする。

（作用）

本発明の電子式入札方式においては、入札者から入札額mに対する圧縮値を作成して開札者に送信し、開札者がすべての入札者から圧縮値を受信して公開した後、入札者は入札額mを開札者に

送信し、これにより開札者が入札額ｍを見た後に不正に入札できないようにしている。開札者はすべての入札額ｍを受信して落札額ｍｏを決定する。また、入札者は圧縮値を開札者に送信する前に身元確認者に身元を確認してもらい、入札額ｍの署名値を求めておき、落札者は前記署名値を開札者に送信し、開札者は落札者の身元が身元確認者によって承認されていることを確認する。身元確認者が署名するのは入札額そのものでなく、入札者のみが知る乱数成分を付加した値であり、入札者はこの乱数成分の影響を除去して入札額に対する署名値を求めている。

（実施例）

以下、図面を用いて本発明の実施例を説明する。

第１図、第２図および第３図は、本発明の一実施例に係わる電子式入札方式に使用される入札者用装置１００、身元確認者用装置２００および開札者用装置３００の構成を示すブロック図をそれぞれ示している。これらの入札者用装置１００、身元確認者用装置２００および開札者用装置３００はそれぞれ第４図に示すように通信回線を介して接続されている。

本実施例に示す電子式入札方式においては、身元確認者が入札者の身元を確認し、この確認を証明する署名を入札者に送信し、入札者が入札額ｍから求めたデータ圧縮値Ｈ（ｍ）を開札者に送信し、開札者がすべての圧縮値Ｈ（ｍ）を公開した後に、入札者が入札額ｍを開札者に送信し、開札者がその値を公開して落札額ｍｏを決定し、落札者が落札額ｍｏに対する署名値を開札者に提示して、開札者が落札者の正当性を認定する。ここで、身元確認者と開札者とが結託しても入札者と入札額の対応を秘密にできるようにするために身元確認者に対して入札額を秘密にしたまま身元確認者に署名されるようにしている。

身元確認者は、ｆ（ｇ（ｘ））＝ｇ（ｆ（ｘ））＝ｘ，ｇ（ｘ×ｙ）＝ｇ（ｘ）×ｇ（ｙ）、かつｆからｇを求めるのが困難な２つの関数の組（ｆ，ｇ）を選択して、関数ｆを公開し、関数ｇを秘密にする。

この性質を満たす関数として、例えばＲＳＡ暗号の暗号化関数と復号化関数がある。ＲＳＡ暗号（Ｒｉｖｅｓｔ，Ｒ．Ｌ．ｅｔａｌ．“Ａ Ｍｅｔｈｏｄ ｆｏｒ Ｏｂｔａｉｎｉｎｇ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅｓ ａｎｄ Ｐｕｂｌｉｃ－Ｋｅｙ Ｃｒｙｐｔｏｓｙｓｔｅｍｓ”，Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ ｏｆ ｔｈｅ ＡＣＭ，Ｖｏｌ．２１，Ｎｏ．２，ｐｐ．１２０－１２６，（１９７８））を用いた（ｆ，ｇ）の構成例は以下の通りである。

身元確認者は暗号化鍵（ｅ，Ｎ）と復号化鍵（ｄ，Ｎ）を

Ｎ＝Ｐ×Ｑ

ｅ×ｄ≡１（ｍｏｄＬ）

但しＬ＝ＬＣＭ｛（Ｐ－１），（Ｑ－１）｝

を満たすように生成し、暗号化鍵を公開し、復号化鍵を秘密に管理する。

ここで、ＬＣＭ｛ａ，ｂ｝は整数ａとｂの最小公倍数を表して、ＰとＱは相異なる２つの大きな素数とする。また、ａ≡ｂ（ｍｏｄＬ）はａ－ｂがＬの倍数であることを表す。

ＲＳＡ暗号は、Ｎが大きいときＮの素因数分解が困難なことに安全性の根拠を持つ暗号であり、公開された暗号化鍵（Ｎ，ｅ）から秘密の復号化鍵のｄ成分を求めることは困難である。

暗号化関数ｆと復号化関数ｇを

ｆ（Ｍ）＝Ｍ^{e}（ｍｏｄＮ）

ｇ（Ｃ）＝Ｃ^{d}（ｍｏｄＮ）

で定義すると、０≦ｘ＜Ｎを満たす整数ｘに対して

ｇ（ｆ（ｘ））＝ｆ（ｇ（ｘ））＝ｘ

が成り立つことを示せる。ここで、ａ（ｍｏｄＮ）は、ａをＮで割ったときの余りを表す。更に、０≦ｘ，ｙ＜Ｎを満たす整数ｘ，ｙに対して

ｇ（ｘ×ｙ）＝ｇ（ｘ）×ｇ（ｙ）

が成り立つことが示せる。

以下では、関数ｇを署名関数として使用し、関数ｆを認証関数として使用する。ｆおよびｇとしてＲＳＡ暗号を用いる場合のｆ計算器とｇ計算器の効率のよい計算方法は、例えば池野、小山による「現代暗号理論」、電子通信学会、ｐｐ．１６－

17、（1986）に示されている。

次に、第5図に示す交信順序例および第1図～第4図を参照して詳細に説明する。

まず、入札者は入札者用装置100の乱数発生器110を使用して乱数Rを生成し、攪乱器120に供給する。該攪乱器120では、関数fを計算するf計算器121を用いて、乱数Rに対するf（R）を算出し、乗算器122に供給する。それから、この乗算器122には入札額mが入力される。乗算器122は、入札額mおよびf（R）を整数と見なし、公開されたNを用いて攪乱された通信文m'を次式により計算する。

$$m' = m \times f(R) \pmod N$$

そして、この計算された通信文m'を身元確認者用装置200に送信する（第5図のステップ110）。なお、この時、入札者－身元確認者間は署名通信を行うとよい。

身元確認者用装置200における身元確認者は入札者用装置100から送信されてきた通信文m'を受信すると、入札者の身元を確認し、それから入札者用装置100からの通信文m'を証明器210に供給する。証明器210は、関数gを計算するg計算器211を用いて通信文m'に対応する署名付き通信文s'を次式により計算する。

$$s' = g(m')$$

それから、この計算した署名付き通信文s'を入札者用装置100に送信する（ステップ120）。

入札者は、入札者用装置100によって身元確認者用装置200からの署名付き通信文s'を乱数成分除去器130で受信する。また、この乱数成分除去器130には、前記乱数発生器110からの乱数Rおよび前記公開されたNが供給されているので、乱数成分除去器130は身元確認者用装置200から受信した署名付き通信文s'、乱数Rおよび公開されたNから次式によって入札額mに対応する署名値sを計算する。

$$s = s' / R \pmod N$$

そして、この計算した署名値sをメモリ140に記憶する。

また、入札者は、入札額mをデータ圧縮器150に供給し、次式により入札額mに対応する圧縮値αを計算する。

$$\alpha = H(m)$$

この計算された圧縮値αを開札者に送信する（ステップ130）。

開札者は、開札者用装置300によって入札者用装置100から送信された圧縮値αを順次受信し、すべての入札者からの圧縮値αを受信すると、その値を公開ファイル310に登録して公開する（ステップ140）。

入札者は、すべての圧縮値αが公開された後、入札額mを開札者用装置300に送信する（ステップ150）。

開札者は、開札者用装置300によって入札者からの入札額mを受信すると、該入札者をデータ圧縮器320に供給し、該データ圧縮器320で圧縮された出力結果が前記公開ファイル310に登録されたいずれかの圧縮値αと一致するか否かを比較器325で比較して検査し、それから入札額mを公開する（ステップ160）。そして、登録されたすべての入札額mから落札額moを決定する。

落札額moを決定された入札者（以下、落札者と称する）は、落札額moに対応する署名値sを前記メモリ140から読み出して開札者用装置300に送信する（ステップ170）。

開札者は、開札者用装置300によって入札者からの署名値sを受信すると、該署名値sを検査器330に供給し、検査値330のf計算器331で該署名値sに対応するf（s）を計算し、この計算されたf（s）を比較器332に供給し、該比較器332において前記落札額moと比較して一致することを検査し、署名値sが落札額moに対応した署名値であることを認定する。

第6図、第7図および第8図は、本発明の他の実施例に係わる電子式入札方式に使用される入札者用装置101、身元確認者用装置201および開札者用装置301の構成を示すブロック図をそれぞれ示している。なお、これらの装置101，201，301はそれぞれ前述した第1図～第3

図に示した装置１００，２００，３００に対応するものであり、該装置１００，２００，３００と共通の構成要素は省略して図示されている。また、前述した第１図～第３図に示す実施例はＲＳＡ暗号を利用するのに対して、この第６図～第８図に示す実施例は、ＦｉａｔとＳｈａｍｉｒの認証方式を利用している。

このＦｉａｔ－Ｓｈａｍｉｒ法は、信頼できるセンタが個人識別情報としてＩＤを用いる利用者に対して、次の手順でｋ個の秘密情報ｓｉ（１≦ｊ≦ｋ）を生成する。ここで、ｋは安全性を定めるパラメータであり、１以上の値である。また、Ｎは公開情報であり、秘密の素数ＰとＱとを用いて、Ｎ＝Ｐ×Ｑと表せる。ｆは一方向性関数であり、公開されている。

すなわち、まず、一方向性関数ｆを用いて、

$$v_j = f(ID, j) \qquad (1 \leq j \leq k)$$

を計算する。

それから、各ｖｊに対してＮの素因数ＰとＱを用いて、

$$s_j = \sqrt{1/v_j} \pmod N$$

を計算する。すなわち、$s_j^2 = 1/v_j \pmod N$となる。

更に、利用者に対してｋ個のｓｊを秘密に発行し、一方向性関数ｆと合成数Ｎを公開する。

（ｍｏｄ Ｎ）における平方根の計算は、Ｎの素因数（ＰとＱ）がわかっているときのみ実行できる。その方法は、例えばＲａｂｉｎ.Ｍ.Ｏ.：“Ｄｉｇｉｔａｌｌｉｚｅｄ Ｓｉｇｎａｔｕｒｅ ａｎｄ Ｐｕｂｌｉｃ－Ｋｅｙ Ｆｕｎｃｔｉｏｎｓ ａｓ Ｉｎｔｒａｃｔａｂｌｅ ａｓ Ｆａｃｔｏｒｉｚａｔｉｏｎ”，Ｔｅｃｈ.Ｒｅｐ.ＭＩＴ/ＬＣＳ/ＴＲ－２１２ ＭＩＴ Ｌａｂ.Ｃｏｍｐｕｔ.Ｓｃｉ.１９７９ に示されている。平方根の計算装置の具体的な構成例は特願昭６１－１６９３５０（公開鍵暗号システム）に開示されている。

また、Ｆｉａｔ－Ｓｈａｍｉｒ法による利用者の認定方式は次の通りである。

証明者Ａは検証者Ｃに対して、Ａが本物であることを次の手順で証明する。

まず、ＡがＩＤをＣに送る。

それから、Ｃは次式を計算する。

$$v_j = f(ID, j) \qquad (1 \leq j \leq k)$$

次に、ｉ＝１，……，ｔについて以下の手順を繰り返す（ｔは安全性を定めるパラメータであり、１以上の値である）。

まず、乱数r_iを生成して、

$$x_i = r_i^2 \pmod N$$

を計算して、Ｃに送る。

それから、Ｃが０，１のビット列（e_{i1}，……，e_{ik}）を生成して、Ａに送る。

更に、Ａが署名文ｙｉを

$$y_i = r_i \prod_{e_{ij}=1} s_j \pmod N$$

で生成して、Ｃに送る。

また、Ｃは、

$$x_i = y_i^2 \prod_{e_{ij}=1} v_j \pmod N$$

が成り立つことを検査する。

y_iの作り方より$y_i^2 \prod_{e_{ij}=1} v_i = r_i^2 \prod_{e_{ij}=1}$（$s_i^2 \times v_i$）$= r_i^2 = x_i \pmod N$であるから、ｔ回の検査にすべて合格した場合、検証者ＣはＡが本物あると認める。

以上では、利用者の認証方式について説明したが、メッセージの認証方式は上記の手順を次のように変更して実現できる。

メッセージ（ｍ）と（x_1，……，x_t）に一方向性関数ｆを施して得たｆ（ｍ，x_1，……，x_t）の先頭のｋｘｔビットを上記手順のビット列（e_{ij}）とみなして、署名文として、（ＩＤ，ｍ，（e_{ij}），y_1，……，y_t）を署名つき通信文として検証者に送信する。

次に、第９図に示す交信順序例および第６図～第８図を参照して詳細に説明する。なお、本実施例では、身元確認者－入札者間ではＦｉａｔ－Ｓｈａｍｉｒ法の利用者認証法を利用し、入札者－開札者間ではＦｉａｔ－Ｓｈａｍｉｒ法のメッセージ認証法を利用している。２つの認証法を対応づける情報を入札者において秘密にすることで、身元確認者と開札者が結託しても入札者と入札額の対応を秘密にしている。

Ｆｉａｔ－Ｓｈａｍｉｒ法の場合と同様に、信頼できるセンタが合成数Ｍと一方向性関数ｆを公開し、更に証明者Ａの識別情報ＩＤに対応する秘密情報ｓを計算して、ｓをＡに配送する。以下の説明では、ｋ＝１の場合について説明する。

入札者は、身元確認者の力を借りて、次の手順で入札額ｍに署名する。

まず、身元確認者は、ＩＤを入札者用装置１０１および開札者用装置３０１に送信する（第９図のステップ２１０）。

それから、身元確認者、入札者および開札者は、それぞれ身元確認者用装置２０１、入札者用装置１０１および開札者用装置３０１のデータ圧縮器２２０，１６０および３５０を用いて、ｘ＝ｆ（ＩＤ）を計算する。

更に、身元確認者は、初期応答文発生器２３０を用いてｔ個の初期応答文ｘ′ｉ（ｉ＝１，２，……，ｔ）からなるｘ′を計算し、この初期応答文ｘ′を入札者用装置１０１に送信する（ステップ２２０）。

なお、初期応答文発生器２３０は、乱数発生器２３１および剰余付き乗算器２３２から構成され、乱数発生器２３１からｔ個のｒｉを発生し、剰余付き乗算器２３２を用いて、

$$x'_i = x \times r_i^2 \pmod N \quad (i = 1, 2, \cdots\cdots, t)$$

で、ｔ個のｘ′ｉを計算する。

前記初期応答文ｘ′が入札者用装置１０１で受信されると、乱数発生器１７０を用いてｔ組のビットｅｉと乱数ｕｉのペアを発生し、その値を受信したｔ個のｘ′ｉと先に生成したｘとともに初期応答文攪乱器１７５に入力し、ｔ個の攪乱された初期応答文ｘ′′ｉを計算してｘ′′＝（ｘ′′１，……，ｘ′′ｔ）を問い合わせ文発生器１８０に供給する。

例えば、初期応答文攪乱器１７５を剰余付き乗算器で構成し、乱数発生器１７０が生成したｔ組のｅｉとｕｉ、受信したｔ個の初期応答文ｘ′ｉおよびｘを剰余付き乗算器１７５に入力し、

$$x''_i = u_i^2 \times x^{-e_i} \times x'_i \pmod N \quad (i = 1, 2, \cdots\cdots, t)$$

でｔ個のｘ′′ｉを計算する。

次に入札者は、入札額ｍとｔ個のｘ′′ｉ入札者用装置１０１の問い合わせ文発生器１８０に入力して、問い合わせ文β，β'を作成し、β'を身元確認者用装置２０１に送信し（ステップ２３０）、βを乱数成分除去器１９０に供給する。

例えば、問い合わせ文発生器１８０をデータ圧縮器１８１および排他的論理和計算器１８２で構成し、これにより

$$(\beta_1, \cdots\cdots, \beta_t) = f(m, x''_1, \cdots\cdots, x''_t)$$

$$\beta'_i = \beta_i + e_i \pmod N \quad (i = 1, 2, \cdots\cdots, t)$$

で、$\beta = (\beta_1, \cdots\cdots, \beta_t)$と

$\beta' = (\beta'_1, \cdots\cdots, \beta'_t)$を求める。

それから、身元確認者用装置２０１は入札者用装置１０１から問い合わせ文β'を受信すると、証明器２４０を用いて、先に発生した乱数ｒｉと受信した問い合わせ文β'から、応答文ｚを計算して入札者用装置１０１に送信する（ステップ２４０）。

例えば、証明器２４０を秘密情報格納器２４１および剰余付き乗算器２４２で構成し、秘密情報格納器２４１から秘密情報ｓを読み出し、初期応答文発生器２３０から供給された乱数ｒと受信した応答文β'を剰余付き乗算器２４２に入力し、

$$z_i = r_i \times s^{\beta'_i} \pmod N \quad (i = 1, 2, \cdots\cdots, t)$$

で計算したｚｉを用いて、ｚ＝（ｚ１，……，ｚｔ）を求める。

入札者用装置１０１が前記応答文ｚを受信すると、該応答文ｚと先に生成したｘとｔ組の（ｅｉ，ｕｉ）を乱数成分除去器１９０に入力し、応答文ｚ′を計算し、応答文ｚ′と問い合わせ分βを入札額ｍに対する署名としてメモリ１４０に記憶する。

例えば、乱数成分除去器１９０を条件判定器１９１および剰余付き乗算器１９２で構成し、

$$\begin{cases} u_i \times z_i \times x^{-1} \pmod N \\ \end{cases}$$

$$z'_i = \begin{cases} (e_i = 1 \text{かつ} \beta_i = 0 \text{のとき}) \\ \\ (i = 1, 2, \cdots\cdots, t) \\ u_i \times z_i \times \quad (\mathrm{mod}\ N) \\ (\text{その他}) \end{cases}$$

で計算したz'_iを用いて、$z' = (Z'_1, \cdots\cdots, z'_t)$を求める。

次は、前述したステップ１３０～１６０と同様に、第９図のステップ２５０～２８０で示すように、入札者は入札額mに対応する圧縮値αを開札者用装置３０１に送信し（ステップ２５０）、開札者はすべての圧縮値αを公開する（ステップ２６０）。それから、入札者はすべての圧縮値αが公開された後、入札額mを開札者用装置３０１に送信する（ステップ２７０）。入札者は入札額mを受信すると、前記公開した圧縮値αと一致するか否かを比較検査し、それからすべての入札額mを公開する（ステップ２８０）。そして、すべての入札額mから落札額moを決定する。

落札者moを決定された入札者、すなわち落札者は、落札額moに対する署名β，z'を前記メモリ１４０から読み出し、開札者用装置３０１に送信する（ステップ２９０）。

開札者は該通信文β、z'を受信すると、該通信文および落札額moを検査器３６０に供給して、これらの正当性を検査する。

この検査器３６０は、例えば剰余付き乗算器３６１、データ圧縮器３６２および比較器３６３で構成され、

$$x''_i = z'_i{}^{2} \times x_i{}^{\beta'} \quad (\mathrm{mod}\ N)$$

でx''_iを求めて、

$$\beta = f(m, X''_1, \cdots\cdots, x''_t)$$

が成立するかを検査する。

以上の実施例では、Ｆｉａｔ－Ｓｈａｍｉｒ法をベースにした認証方法について説明したが、Ｆｉａｔ－Ｓｈａｍｉｒ法はＮの素因数分解が困難な場合に（ｍｏｄ Ｎ）での平方根の計算が困難なことに基づいている。離散対数問題などの困難性を利用した認証法をベースにしても同様の方式を構成できる。

［発明の効果］

以上説明したように、本発明によれば、入札者は入札額mから圧縮値を作成して開札者に送信し、開札者がすべての入札者から圧縮値を受信して公開した後に開札者が入札額mを開札者に送信しているので、開札者が入札額mを見た後に不正に入札できない。また、落札者のみが署名値を開札者に送信して、落札者の身元を承認するので、落札額以外の入札額と入札者との対応関係を秘密にできる。特に、身元確認者が署名するのは、入札額そのものでなく、入札者のみが知る乱数成分を付加した値であり、入札者はその乱数成分の影響を除去して入札値に対する署名値を求めるので、入札の主催者である身元確認者と開札者とが結託しても落札者と落札額以外の入札額mと入札者との対応関係を秘密にすることができ、入札主催者による不正行為、入札額の漏洩などを防止することができる。

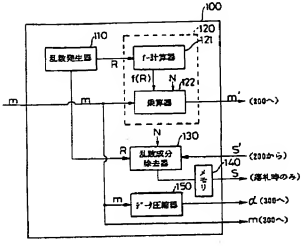
４．図面の簡単な説明

第１図、第２図および第３図は本発明の一実施例に係わる電子式入札方式に使用される入札者用装置、身元確認者用装置および開札者用装置の構成をそれぞれ示すブロック図、第４図は電子式入札方式において通信ネットワークを介して接続される身元確認者、入札者および開札者を示す図、第５図は第１図～第３図の実施例における交信順序を示す説明図、第６図、第７図および第８図は本発明の他の実施例に係わる電子式入札方式に使用される入札者用装置、身元確認者用装置および開札者用装置の構成をそれぞれ示すブロック図、第９図は第６図～第８図の実施例における交信順序を示す説明図である。

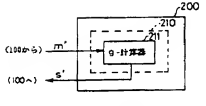
１００，１０１…入札者用装置
１１０…乱数発生器
１２０…撹乱器
１７０…乱数成分除去器
１４０…めもり
１５０…データ圧縮器
２００，２０１…身元確認者用装置
２１０…証明器

３００，３０１…開札者用装置
３１０…公開ファイル
３２０…データ圧縮器
３３０…検査器

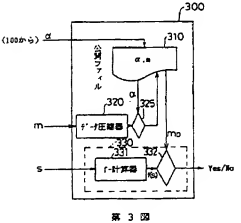
代理人　弁理士　三　好　保　男



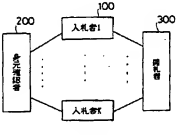
第１図



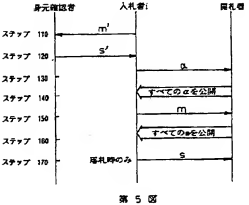
第２図



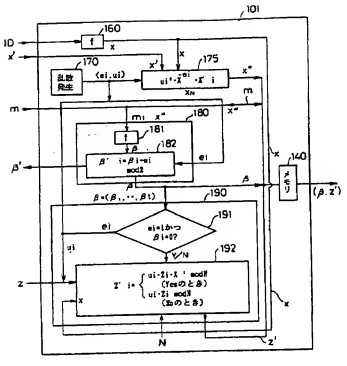
第３図



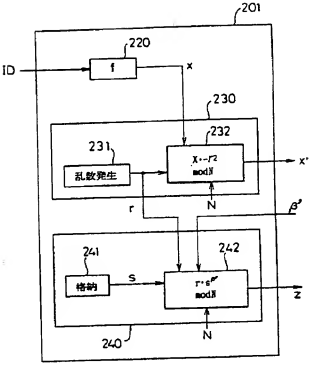
第４図



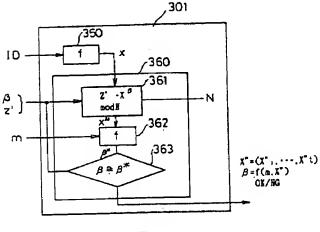
第５図



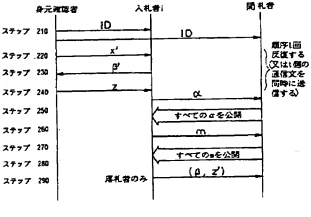
第 6 図



第 7 図



第 8 図



第 9 図

手 続 補 正 書（自発）

昭和 63年 11月10日

特 許 庁 長 官 殿

63-272605

1．事件の表示　昭和６３年１０月２８日に提出した特許願（３）

2．発明の名称　電子式入札方式

3．補正をする者
事件との関係　特許出願人
住所（居所）　東京都千代田区内幸町１丁目１番６号
氏名（名称）　（422）日本電信電話株式会社
代表者　山 口 開 生

4．代 理 人
住 所　〒105 東京都港区虎ノ門１丁目２番３号
虎ノ門第１ビル５階
電話　東京（ 504）3075（代）
氏 名　弁理士（8834）三 好 保 男

5．補正の対象
(1) 明細書

6．補正の内容
(1) 明細書の浄書。別紙のとおり（内容に変更なし）。

以 上

特許庁 63.11.10 出願第二係